## PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to convey passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of MDHHS' entire corporate network. As such, MDHHS workforce members (including contractors and vendors with access to MDHHS systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## REVISION HISTORY

Issued: 09/20/2006

Reviewed: 01/01/2016

Revised: 01/01/2016

## DEFINITIONS

**ePHI** is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

**PHI** is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

**Workforce Member** means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

**One-Time Tokens** are dynamic passwords which are only used once and become ineffective immediately after use.

## POLICY

It is the policy of the MDHHS to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change. This policy includes all personnel who have or are responsible for an account (or any form of access that

supports or requires a password) on any system that resides at any MDHHS facility, has access to the MDHHS network or stores any non-public MDHHS information.

## PROCEDURE

### Department of Technology, Management and Budget (DTMB)

DTMB must on a periodic or random basis perform password cracking or guessing. If a password is guessed or cracked during one of these scans notify the user and the user will be required to change the password immediately.

### Workforce Member

Workforce members must:

- Select strong passwords. See characteristics of strong passwords in the Tips and Hints section.
- Change user level passwords at least every sixty days and system level passwords every six months.
- Report if an account or password is suspected to have been compromised to MMDHHS Security Officer and change all passwords immediately.
- Be aware of how to select strong passwords.
- Never store online or write down passwords. Do not store passwords in a file on **any** computer system (including Palm Pilots or similar devices) without encryption.
- Do not use the remember password feature of applications (such as Eudora, Outlook, web browsers, etc.).
- Never use the same password for MDHHS accounts as for other non-MDHHS access (for example personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various MDHHS access needs.
- Never share MDHHS passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential MDHHS information.

If someone demands a password, refer them to this document or have them contact the DTMB Client Service Center.

Do not use the remember password feature of applications (such as Eudora, Outlook. Netscape Messenger, etc.).

**Tips and Hints:**

Passwords are used for various purposes at MDHHS. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password and local router logins. Very few systems have support for one-time tokens.

Poor, weak passwords have the following characteristics:

- The password contains less than eight alphanumeric characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "MMDHHS", "Lansing" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (such as secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (for example, a-z, A-Z)
- Have digits and punctuation characters as well as letters (for example, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Are at least eight alphanumeric characters in length
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

**Note:** Do not use either of these examples as passwords!

- All system-level passwords (for example root, enable, NT admin, application administration accounts, etc.) must be changed at least every six months.
- All user-level passwords (for example email, web, desktop computer, etc.) must be changed at least every sixty days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described above.

Here is a list of don’ts:

- Don't reveal a password over the phone to **anyone**.
- Don't reveal a password in an email message.
- Don't reveal a password to your supervisor.
- Don't talk about a password within audible range of others.
- Don't hint at the format of a password (for example "my family name").
- Don't reveal a password on questionnaires or security forms.

- Don't share a password with family members.
- Don't reveal a password to coworkers while on vacation.

## REFERENCES

45 CFR 164.308(a)(5)

## CONTACT

For additional information concerning this policy and procedure, contact DTMB Client Service Center at 517-241-9700 or 800-968-2644 or MDHHS Security Officer at MDHHSPrivacySecurity@michigan.gov